E-PRIVACY 2011

L'importanza della qualità nel Web di Dati: modello di sicurezza e privacy per l'*e-profile*.

Ing. Stefano Turchi
Dott. Ing. Maria Chiara Pettenati
Dott. Ing. Lucia Ciofi

Prof. Franco Pirri
Prof. Dino Giuli

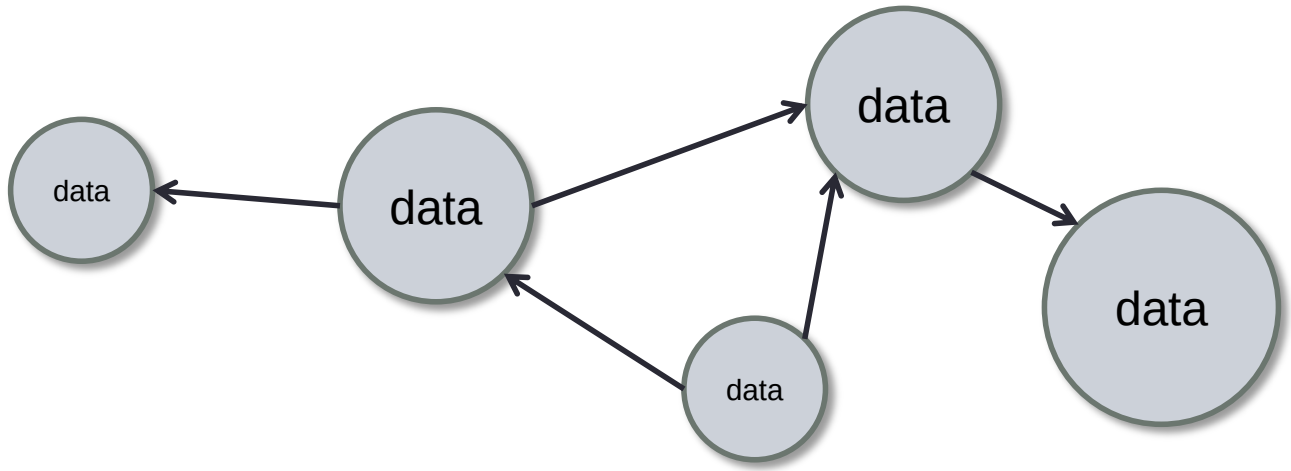
Università degli Studi di Firenze
Dipartimento di Elettronica e Telecomunicazioni

Outline

- Dati e Aggregati di Dati
  - Domande Aperte
- L'Identità Digitale e l'e-profile
- InterDataNet
  - Information Model
  - Architettura
- Background Tecnologico
  - OpenID
  - OAuth
  - Contextual Tree
- La proposta InterDataNet
  - Security Injection
  - Il Protocollo di Autorizzazione
  - Implementazione

Web di Dati

- È il nome dato ad una delle direzioni evolutive del prossimo Web e si riferisce alla possibilità di pubblicare ed interconnettere informazioni.



- Le informazioni (dati) sono tanto più **utili** quanto più **granulari**!

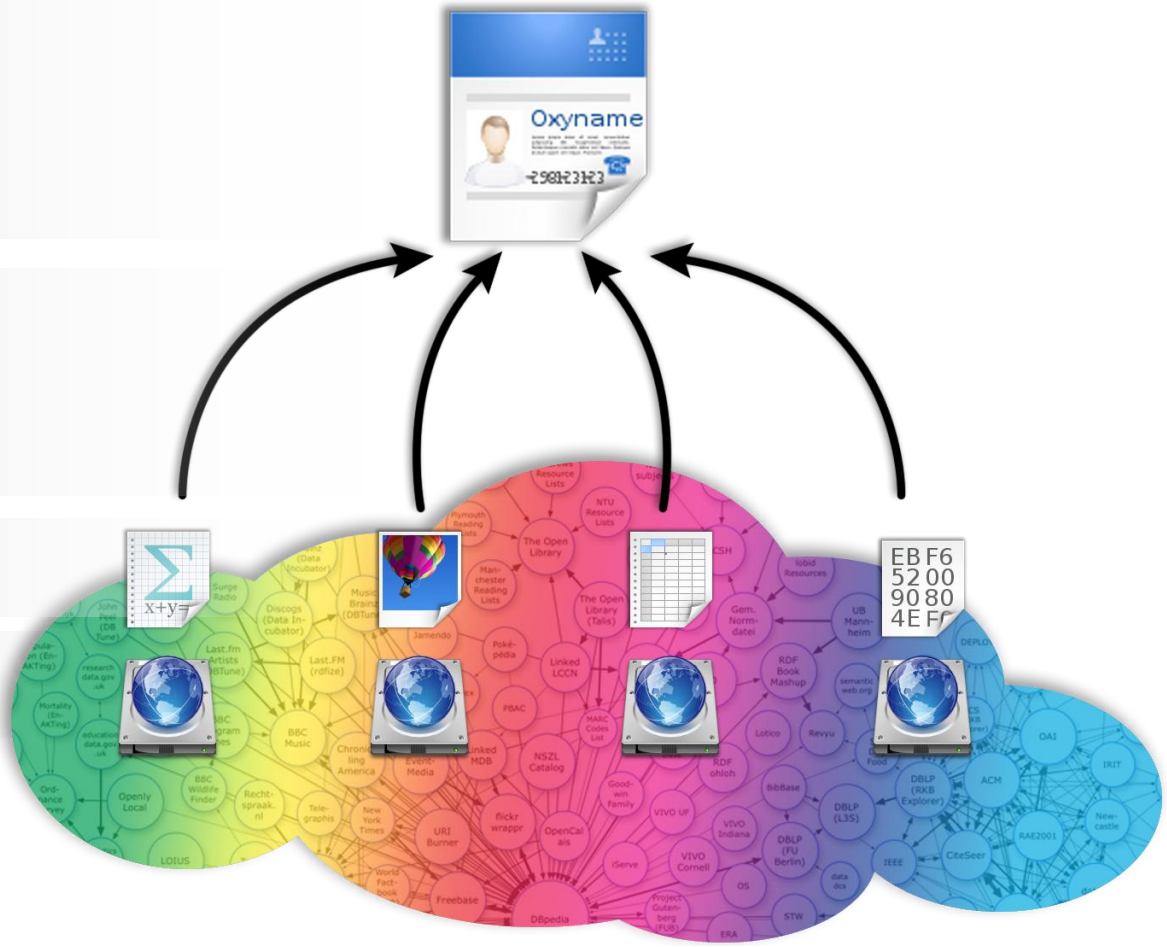
Dati ed Aggregati di Dati

Documento

Aggregazioni

Dati

Sorgenti di Dati

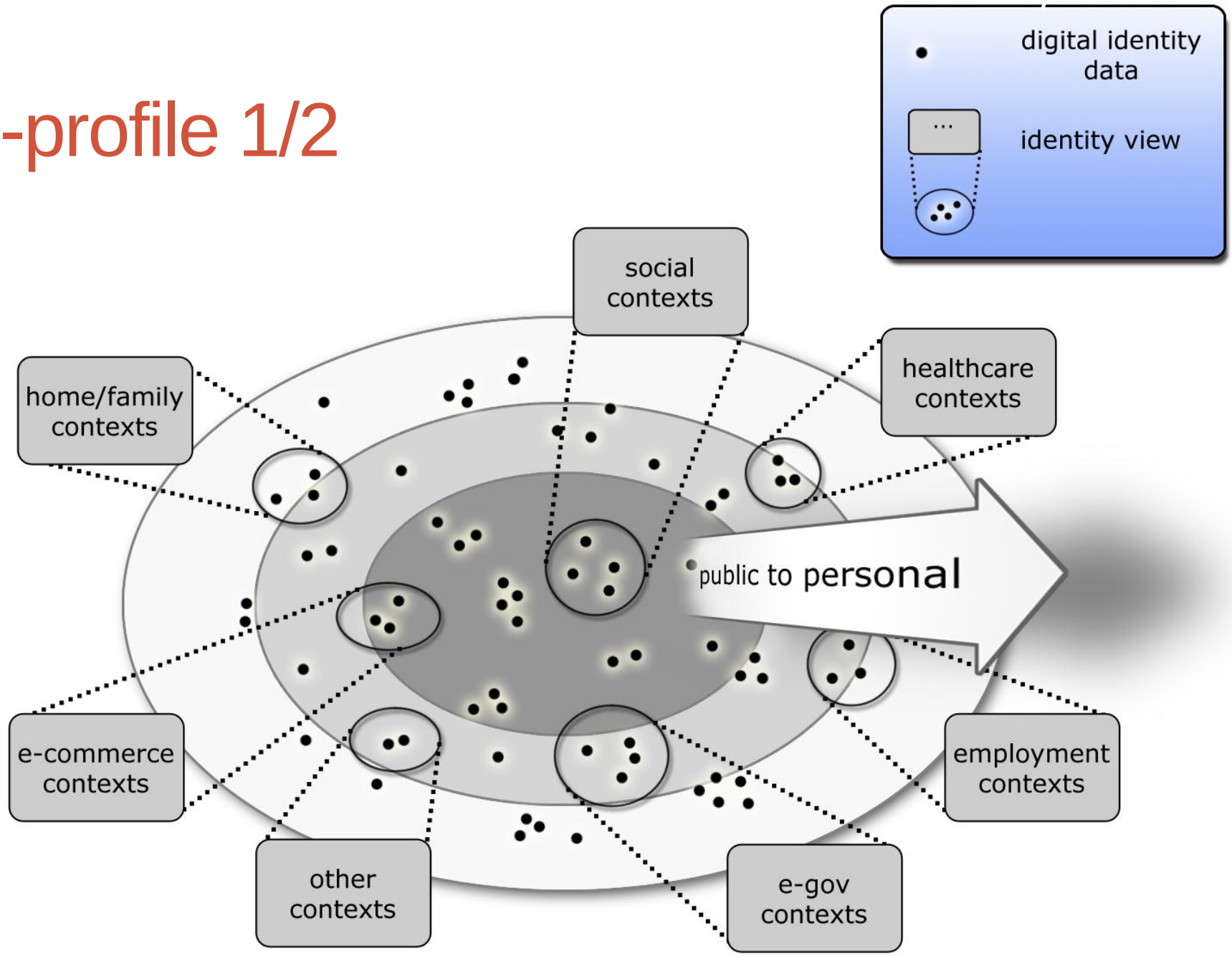


Domande Aperte

- In uno scenario in cui i dati sono riutilizzati intensivamente sorgono problematiche sulla loro qualità:
- Le sorgenti di dati possono essere:
  - Note e fidate
  - Note e non fidate
  - Ignote
  - …?
- Quali proprietà possiede un dato generato aggregando dati eterogenei?
- Come quantificane il livello di sicurezza?
- Come tutelare la privacy?

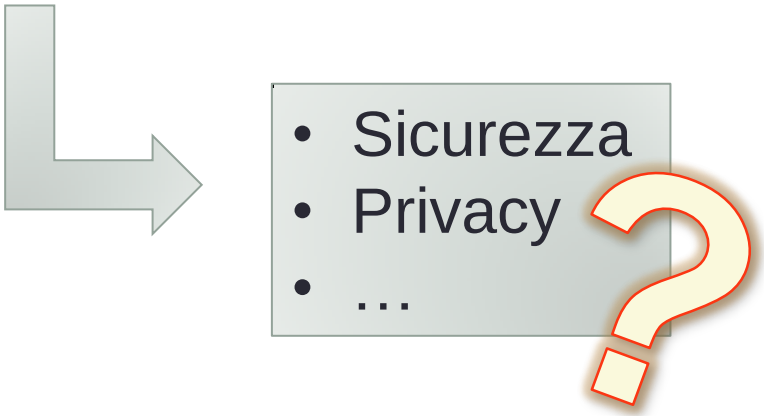
Digital Identity

e-profile 1/2


digital identity data
identity view
social contexts
healthcare contexts
home/family contexts
public to personal
e-commerce contexts
employment contexts
other contexts
e-gov contexts

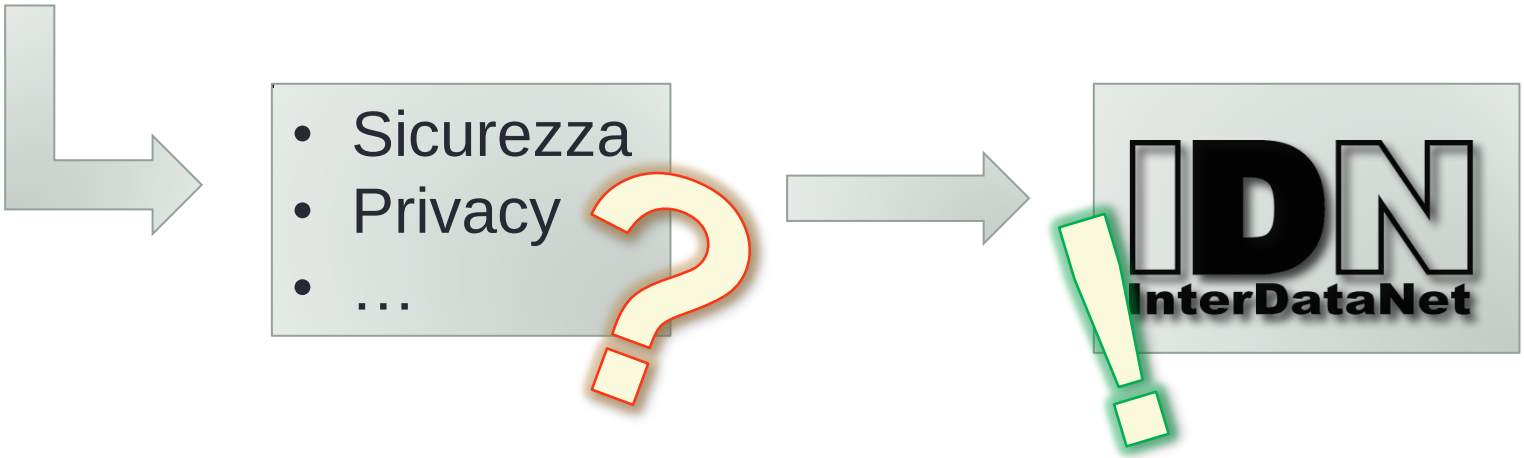
e-profile 2/2

1. I dati che costituiscono il profilo di uno user sono *in the cloud*
2. Le applicazioni accedono a delle viste di sottoinsiemi dell'e-profile



e-profile 2/2

1. I dati che costituiscono il profilo di uno user sono *in the cloud*
2. Le applicazioni accedono a delle viste di sottoinsiemi dell'e-profile



InterDataNet

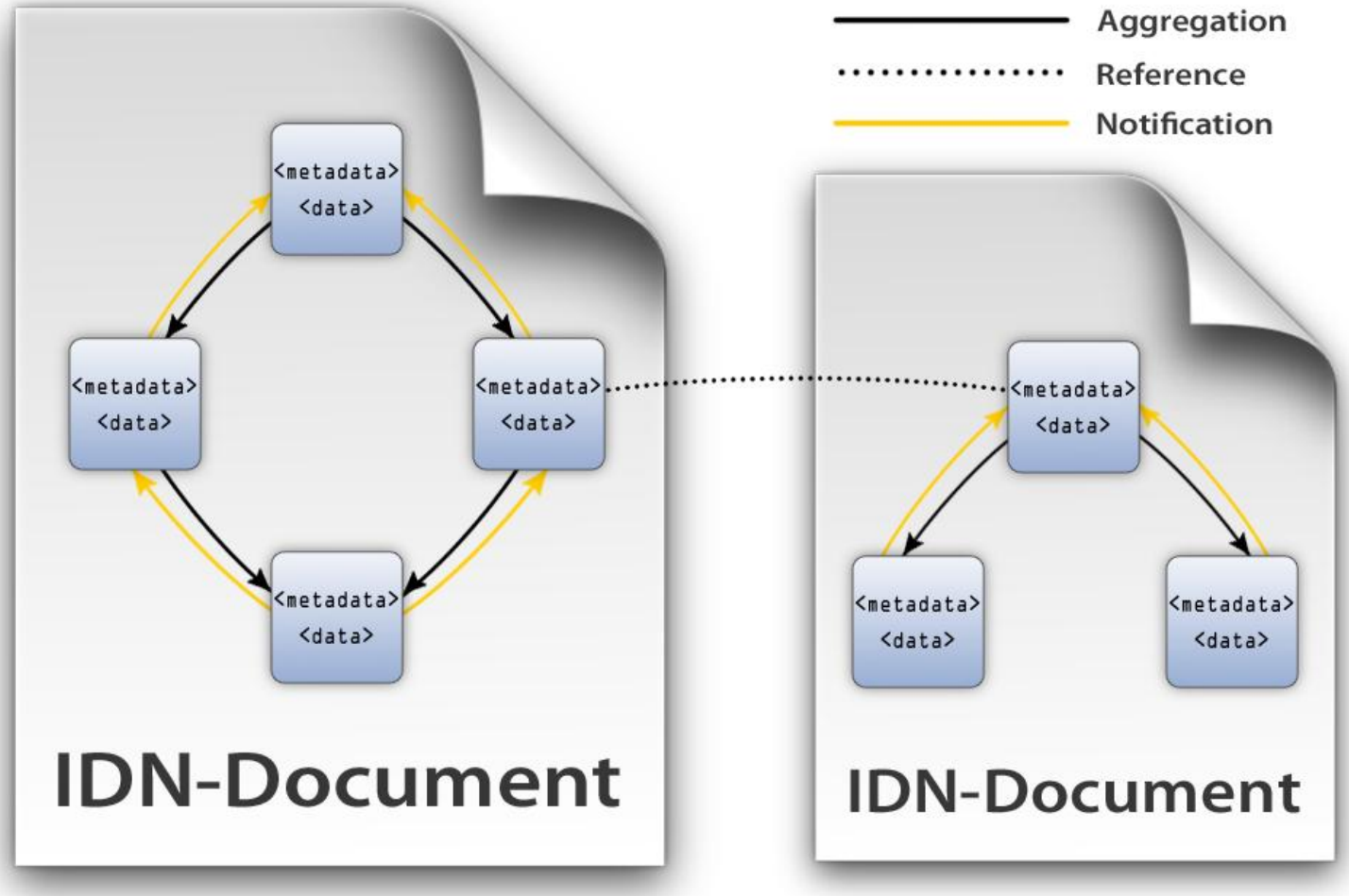
Cos'è	Cosa non è
Un'architettura	Il Web
Una Overlay Network	Una Web Application

Cosa fa	Cosa non fa
Gestisce dati granulari	Un semplice mash-up
Consente di aggregare dati granulari in documenti	
Consente di collaborare intorno a documenti	
Abilita privacy, security, licensing, trust, provenance, versioning, availability sui dati granulari	

Information Model 1/3

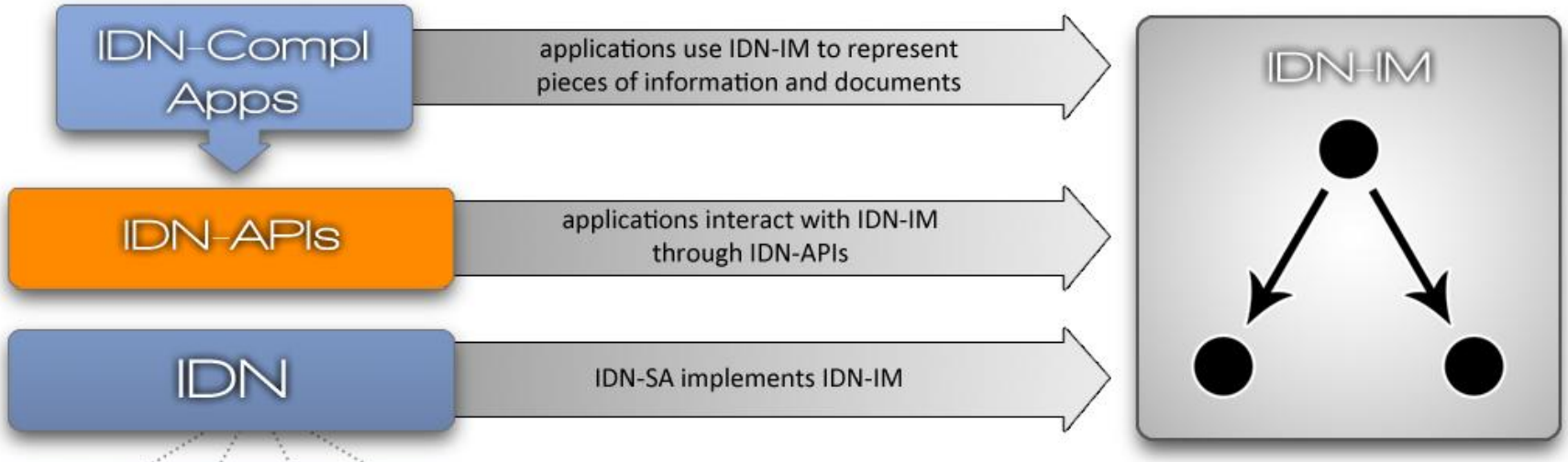
- È il modo in cui IDN rappresenta e gestisce l'informazione
- 2 elementi fondamentali:
  - **Nodi**: costituiscono un frammento informativo
  - **Documenti**: composizioni di più elementi
- 3 relazioni
  - Aggregazione
  - Riferimento
  - Notifica

Information Model 2/3

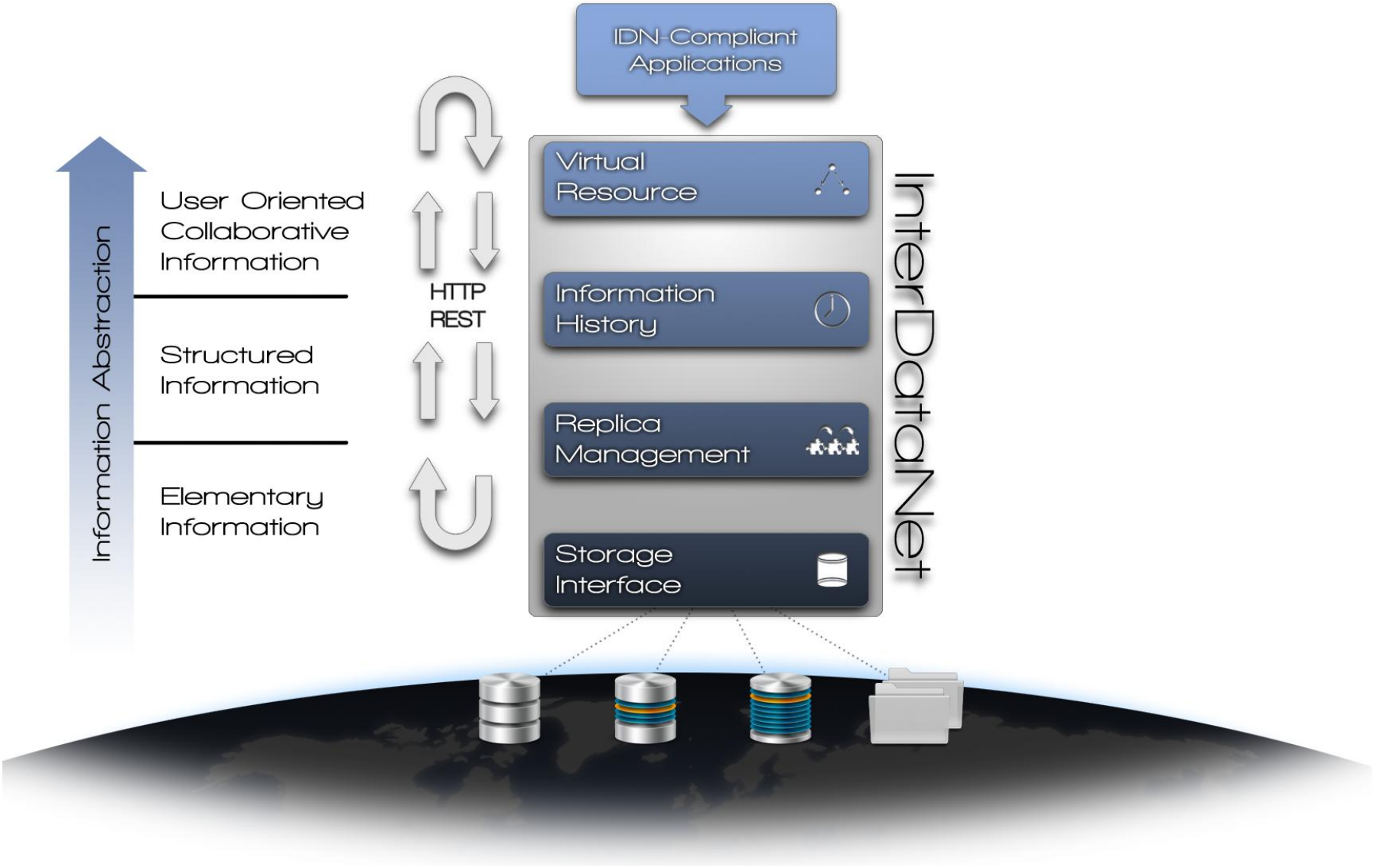


Information Model 3/3

Le applicazioni utilizzano IDN rappresentando l'informazione secondo l'IDN-IM. IDN è completamente agnostico circa la semantica dei dati trattati. Per questo motivo IDN è un'architettura che può essere utilizzata in innumerevoli ambiti diversi!

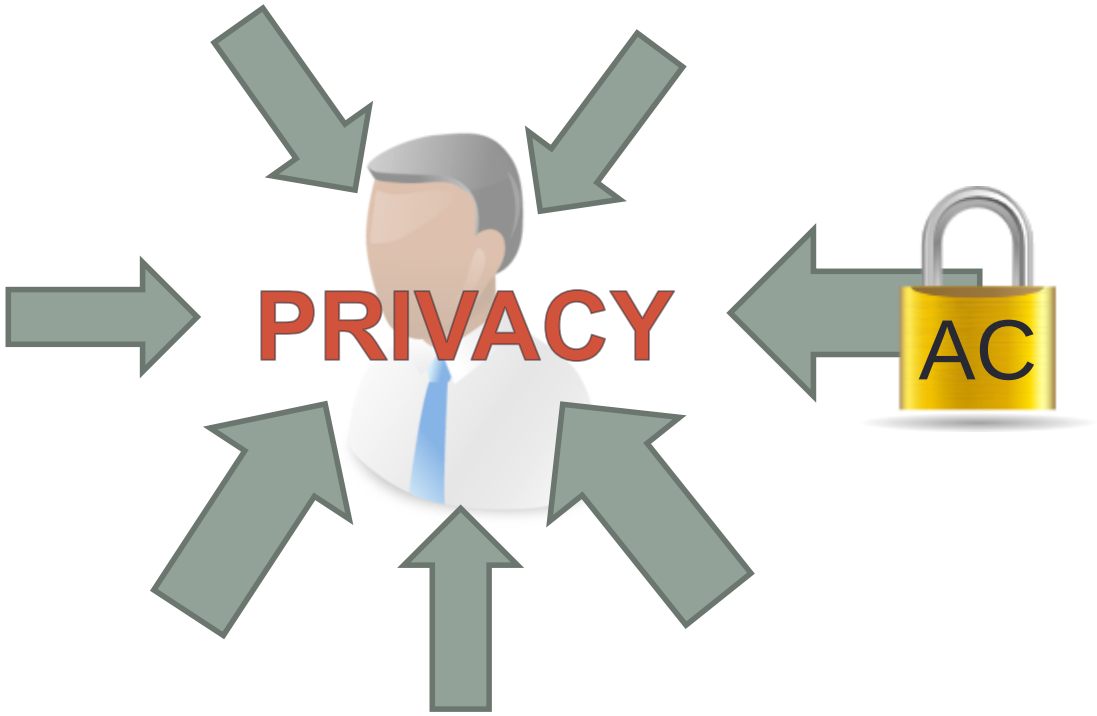


InterDataNet



Privacy e Controllo degli Accessi

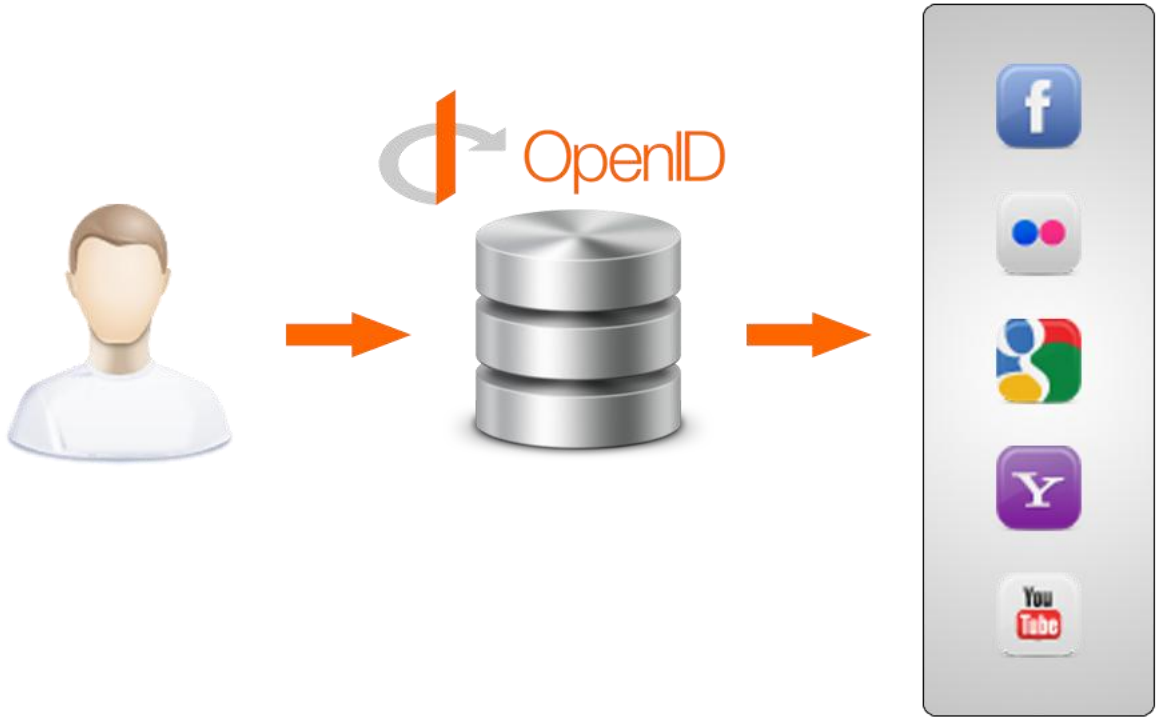
- Il problema della tutela della privacy è senza dubbio complesso e articolato. La soluzione deve arrivare attraverso approcci diversi e cross-disciplinari…



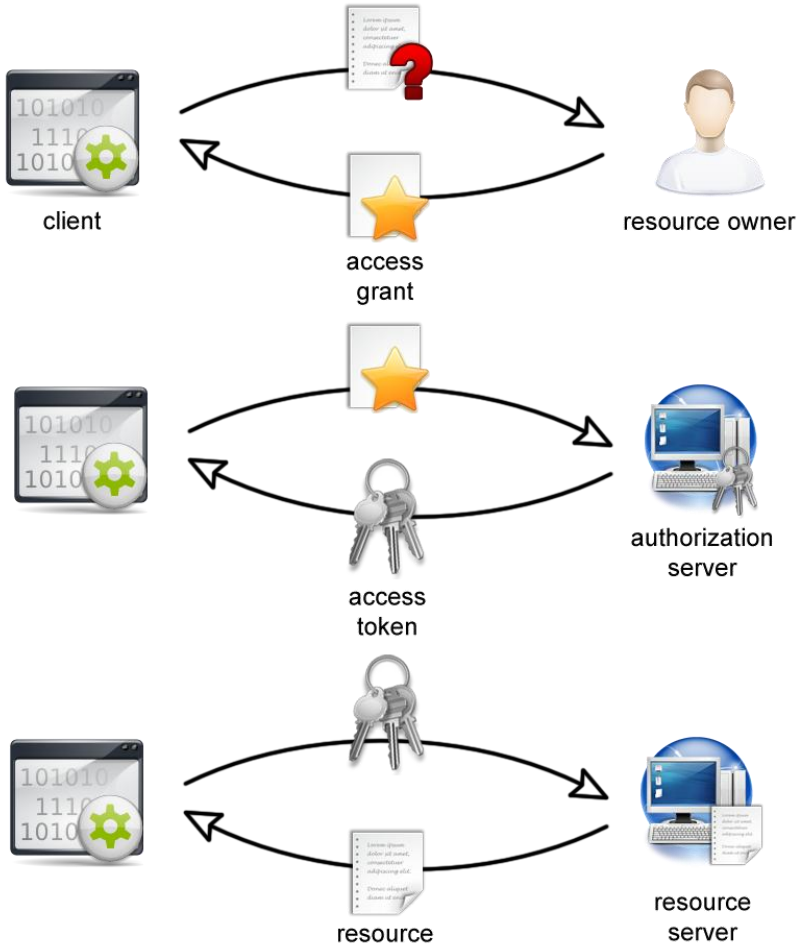
Un elemento determinante è il controllo degli accessi!

IDN e AC: background

- L'identità è associata ad un URL
- La password di un utente è comunicata solo ad OpenID
- OpenID [1] conferma l'identità dell'utente al servizio web



IDN e AC: background



OAuth [2] è un protocollo che consente di interagire con i dati del soggetto, previa autorizzazione

Entità	ruolo
Res. Owner	Il proprietario della risorsa R
Client	Chi effettua la richiesta di accesso ad R
Auth. Server	L'entità che concede il token di accesso
Res. Server	L'entità che ospita R.

Un paradigma noto

- Un utente utilizza un servizio Web
- L'utente consegna i propri dati al servizio Web
- Il servizio Web si assume l'incombenza di proteggere i dati dell'utente
- L'utente si FIDA del servizio Web

Se il dato è tratto dai confini del servizio Web non è più possibile proteggerlo!

Security Injection

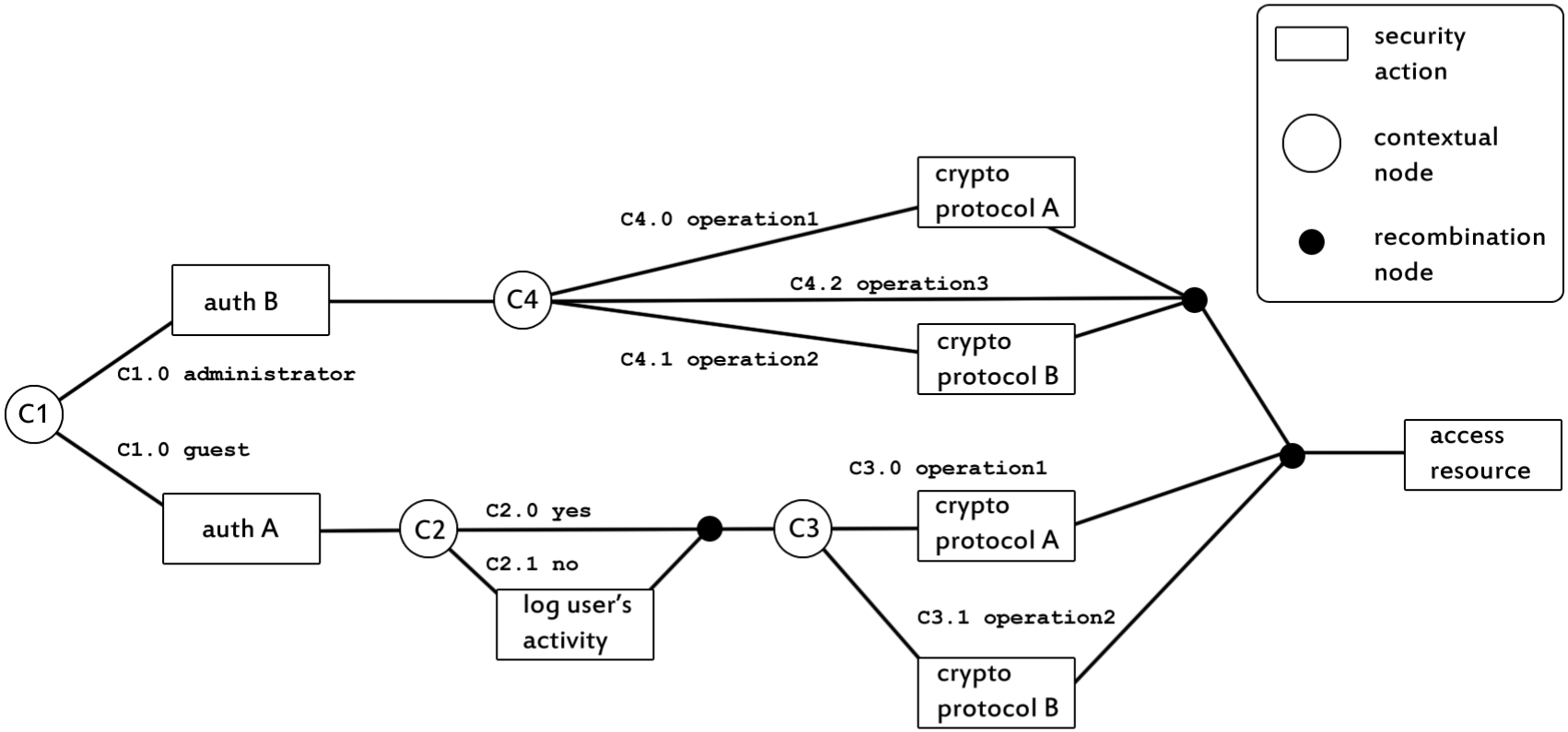
La sicurezza ed altre proprietà sono iniettate all'interno del dato stesso e definite come suoi attributi. In questo modo il dato godrà di una sicurezza «embedded» che non dipenderà dalla propria locazione.

La responsabilità dell'attuazione della politica di sicurezza trasla dall'applicazione all'architettura!

Contextual Graph 1/2

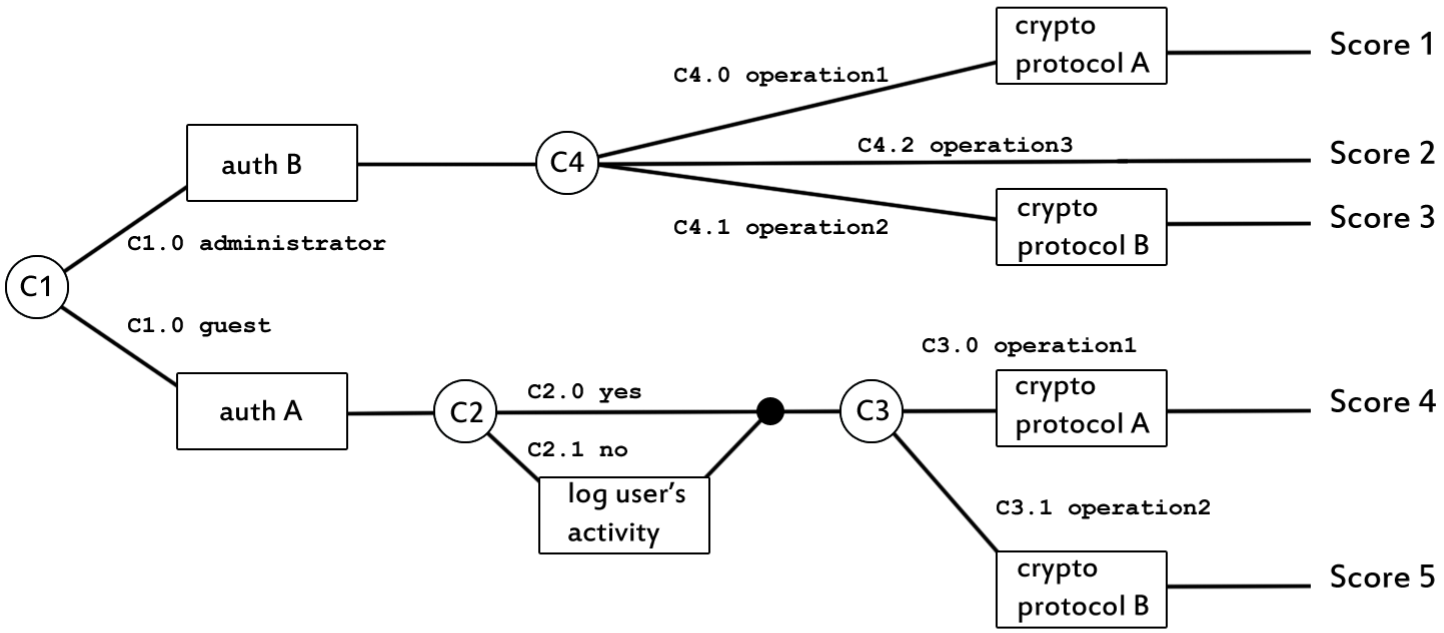
- Si tratta di grafi aciclici utilizzati nel contesto del Pervasive Computing (PC)
- PC necessita di nuove politiche di sicurezza che siano adattive e riconfigurabili a *runtime* (formalmente si parla di contesti)
- I Contextual Graph [3, 4] rappresentano un formalismo per la modellazione di tali politiche.

Contextual Graph* 2/2



* Grafico tratto da [4]

IDN e Contextual Tree



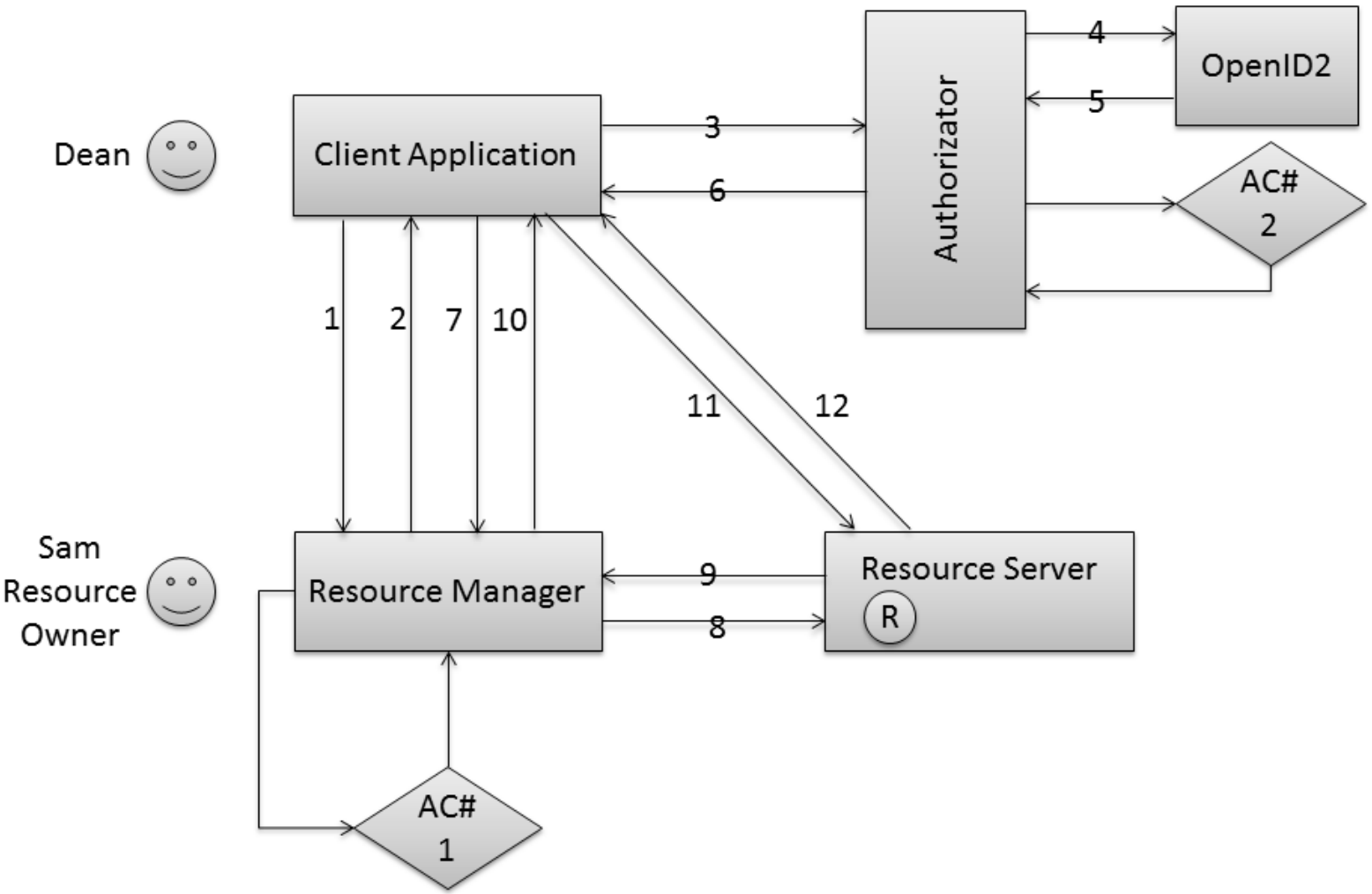
Security Policy 1/2

- Ogni percorso lungo un Contextual Tree dà luogo ad uno score s
- Sia c un contesto
- Sia T una soglia
- Deve essere progettata una funzione $f(c)$ tale che:
  - Se $f(c) = s \geq T \rightarrow$ go on
  - Se $f(c) = s < T \rightarrow$ STOP!

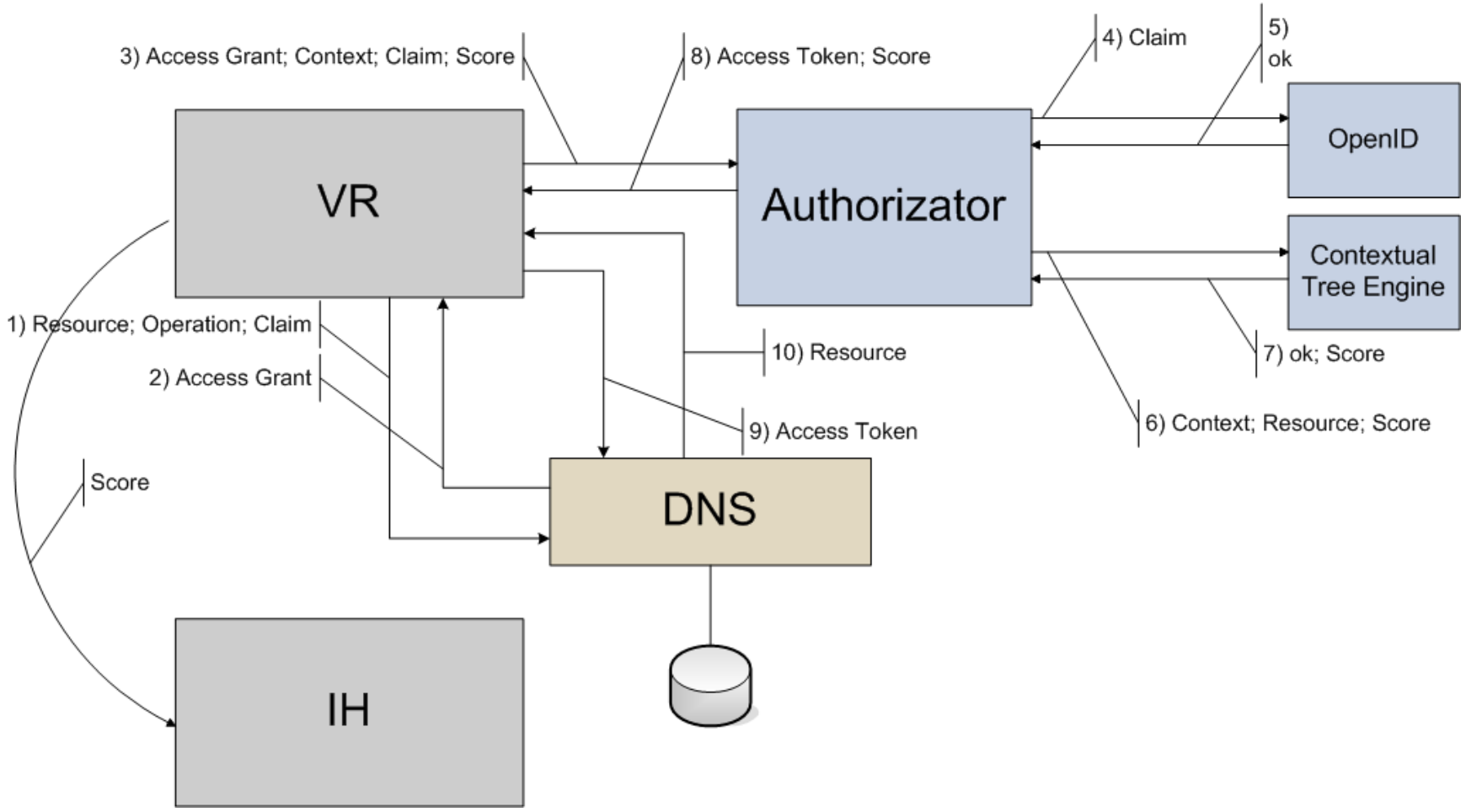
Security Policy 2/2

- Attraverso l'impiego dei Contextual Tree è possibile distribuire la responsabilità sui livelli di IDN coinvolti…
- …ma in che modo gestire la Security come attributo del dato?
- Una nuova soglia D è contenuta nel dato
- Riapplicando il ragionamento precedente si definisce una nuova funzione g tale che:
  - Se $g(f_1(s_0, c_1), \dots, f_n(s_{n-1}, c_n) \geq D \rightarrow$ access granted
  - Se $g(f_1(s_0, c_1), \dots, f_n(s_{n-1}, c_n) < D \rightarrow$ access denied

Il Protocollo di Autorizzazione

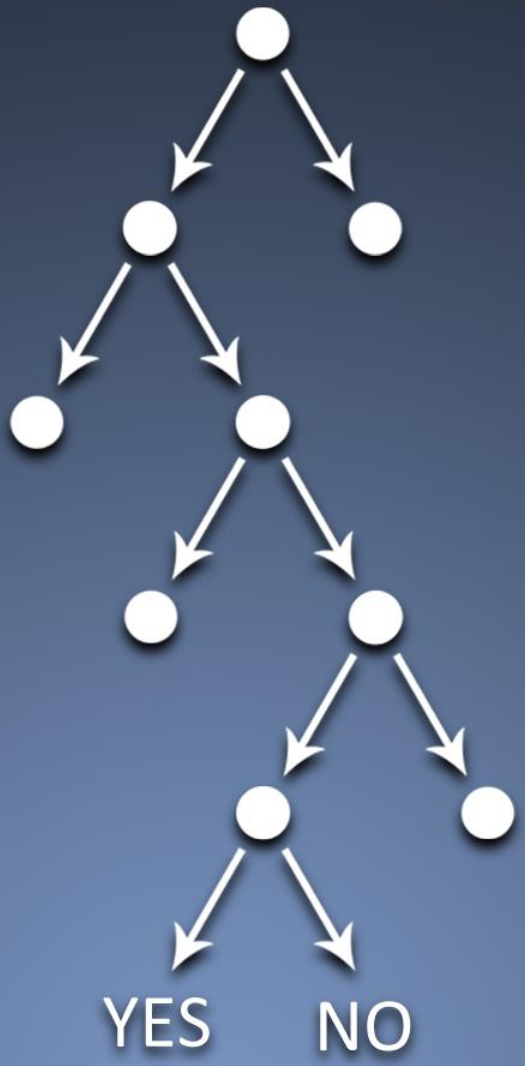


Implementazione del Protocollo in IDN



InterDataNet

Security Policy



grazie per l'attenzione!

IDN
InterDataNet

Contatti: stefano.turchi@unifi.it

Approfondimenti: http://www.interdatanet.org
http://telematicsys.det.unifi.it

Reference

- **[1]** - http://openid.net/
- **[2]** - http://oauth.net/
- **[3]** - Brezillon, P. (2003). Context-based modeling of operators' practices by contextual graphs. In Human Centered Processes: 14th Mini Euro Conference.
- **[4]** - Mostefaoui, G.K., P. Brezillon, "Modeling context-based security policies with contextual graphs," in the Proc. of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, pp. 28-32, 2004.